Dc3 Digital Forensics Challenge

104 – Signature Analysis

Team Information

Team Name:	AWGN		
Results Email:	[redacted]		
Examination Time Frame:	5/21/08	to	5/22/08

Instructions

Description: Examine the files in the **104_Signature_Analysis_Challenge2008** folder to determine which files are using the proper signature information and filename display and which are not. Report the full filename for mismatched files, a detailed explanation of your process (software or technique) used to examine and determine your results, and provide the corrected file.

Points will be awarded for each successfully identified signature mismatch and reasoning for your decision.

Total Weighted Points: **10 Total Points available per entry – Total 100 Points Available**

1. **Answers** – Fill in the chart below with your findings. *As a Forensic Challenge, consider that your answers will have to have enough detail for the Findings and Methodology of your examination to satisfy questioning in a court of law.*
2. **Methodology** – Provide a meticulously detailed explanation of your process. Be sure to include a step action that our reviewers can follow to reproduce your work for authenticity including tools and techniques.

Internal Reviewer Use Only

Reviewer:		Points Awarded:	
Date:		Review Period:	to
Completed:	□ Yes □ No □ Partial		

Report of Examination

Challenge Number: 104 - Signature Analysis

Examiner: Graham Eschbacher

104 Results

Correct Files - Identified by Linux 'file' command

245.JPG Identified by Linux 'file' command
249.JPG Identified by Linux 'file' command
255.JPG Identified by Linux 'file' command
AutoWire.bmp Identified by Linux 'file' command
Bluestar.gif Identified by Linux 'file' command
Chaff_Floral_1179.bmp Identified by Linux 'file' command
Chaff_Landscape_158.gif Identified by Linux 'file' command
Chaff_Landscape_161.gif Identified by Linux 'file' command

Incorrect files - Identified by Linux 'file' command

blank.jpg -> blank.asp
blue.jpg -> blue.asp
CLOCK.MOV -> CLOCK.CAB
DollL Sales Worldwide.html -> DollL Sales Worldwide.jpg
intro.mpeg -> intro.zip
straightline.tif -> straightline.asp

Incorrect files - identified by other means

pctools.zip -> pctools.cat detected by Linux 'file' command,
identified on http://www.garykessler.net/library/file_sigs.html
by searching for first 2 bytes
SYSTEM.1ST -> SYSTEM.dat detected by Linux 'file' command,
identified on http://www.garykessler.net/library/file_sigs.html
by searching for first 4 bytes
SAILBOAT.JPG -> SAILBOAT.chm detected by Linux 'file' command,
identified on http://www.garykessler.net/library/file_sigs.html
by searching for first 4 bytes
Windows.wav -> Windows.cnt detected by Linux 'file' command,
identified with Google search of "WIN_HELP_AUTOCLOSE"

Methodology / Notes Form

Challenge Number: 104 - Signature Analysis

Tool Information

Type	Name	Publisher
○ Commercial ● Open Source	Linux	
○ Commercial ● Open Source	Notepad++ & Hex Viewer plugin	http://notepad-plus.sourceforge.net
○ Commercial ○ Open Source		
○ Commercial ○ Open Source		
○ Commercial ○ Open Source		

Notes

The 'file' command in Linux is used to determine a file's type. This was used to identify if each file has an incorrect extension by telling what type of file it is. It doesn't give the correct extension, but the info it gives is usually enough to identify the correct one through experience or an internet search of the type. When the provided type was vague, then the website http://www.garykessler.net/library/file_sigs.html usually provided the extension according to the file's header. These failed in one case where the given file was in plain text, and contained keywords that appeared to be unique to that type of file. A Google search of this keyword provided the correct extension.

Page 1 of 1